Contenido

Introducción

Una fuente que no es Cisco ha lanzado un programa para descifrar contraseñas de usuarios (y otras contraseñas) en archivos de configuración Cisco. El programa no descifrará contraseñas definidas con el comando enable secret. EIEE 'El interés inesperado que este programa ha causado entre los clientes de Cisco nos ha llevado a sospechar que muchos clientes confían en que el encripción de contraseñas de Cisco les brindará mayor seguridad de la que fue diseñado para brindar. Este documento explica el modelo de seguridad subyacente a la encripción de contraseña de Cisco, y las limitaciones de seguridad de esa encripción.

Nota: Cisco recomienda que todos los dispositivos Cisco IOS implementan el modelo de seguridad del Authentication, Authorization, and Accounting (AAA). AAA puede emplear bases de datos locales, RADIUS y TACACS+.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

Convenciones

Para obtener más información sobre las convenciones del documento, consulte las Convenciones de Consejos Técnicos de Cisco.

Contraseñas de usuarios

Las contraseñas de usuario y la mayoría de las otras contraseñas (excepto las de activar contraseña secreta) en archivos de configuración IOS de Cisco se cifran utilizando un esquema que es muy débil mediante normas criptográficas modernas.

Aunque Cisco no distribuya un programa del desciframiento, por lo menos dos diversos programas del desciframiento para las contraseñas del Cisco IOS están disponibles para el público en Internet; la primera difusión pública de tal programa cuyo Cisco es consciente era a principios de 1995. Esperaríamos que cualquier criptógrafo amateur pudiera crear un nuevo programa con poco esfuerzo.

El esquema utilizado por Cisco IOS para las contraseñas de usuario nunca fue pensado para resistir un ataque inteligente determinado. El esquema de encripción se diseñó para evitar el robo de contraseñas a través de la simulación o el rastreo simple. Nunca fue pensado para proteger contra alguien que conducía un esfuerzo contraseña-que se quebraba en el archivo de configuración.

Debido al algoritmo de encripción vulnerable, ha sido siempre la posición de Cisco que los clientes deben tratar cualquier archivo de configuración que contiene las contraseñas como información vulnerable de la misma forma que tratarían una lista cleartext de contraseñas.

enable secret y enable password

El comando enable password debe ser utilizado no más. Utilice el comando enable secret para mayor seguridad: El único caso en el cual el **comando enable password** pudo ser probado es cuando el dispositivo se está ejecutando en un modo de arranque que no apoye el **comando enable secret**.

Los comandos enable secrets se fragmentan mediante el algoritmo MD5. Según la información que tenemos en Cisco, es imposible recuperar un habilitar secreto basado en los contenidos de un archivo de configuración (a no ser por medio de ataques obvios al diccionario).

Nota: Esto se aplica solamente a las contraseñas fijadas con el **secreto del permiso**, y *no a las* contraseñas fijadas con la **contraseña habilitada**. De hecho, la fuerza del cifrado usado es la única diferencia significativa entre los dos comandos.

¿Qué imagen de Cisco IOS admite enable secret?

Observe su imagen de inicio usando el comando show version desde su modo normal de funcionamiento (imagen completa del IOS de Full Cisco) para ver si la imagen de inicio admite el comando enable secret. Si hace, quitar la **contraseña habilitada**. Si la imagen de inicio del sistema no admite el comando enable secret, observe las siguientes advertencias:

- La determinación de una contraseña habilitada pudo ser innecesaria si usted tiene Seguridad física de modo que nadie pueda recargar el dispositivo a la imagen del arranque de sistema.
- Si alguien tiene acceso físico al dispositivo, puede trastornar fácilmente la seguridad del dispositivo sin necesidad de acceder a la imagen de inicio.
- Si predetermina el enable password a la misma del enable secret, hará que el enable secret esté tan propenso a ataques como el enable password.

- Si configura habilitar contraseña a un valor diferente porque la imagen de reinicio no admite enable secret, los administradores del router deben recordar una nueva contraseña que se use poco en los ROM que no admiten el comando enable secret. Teniendo una contraseña habilitada separada, los administradores pueden no recordar la contraseña cuando están forzando el tiempo muerto para una actualización del software, que es la única razón para iniciar sesión al modo de arranque.

Otras contraseñas

Casi todas las contraseñas y otras cadenas de la autentificación en los archivos de configuración del Cisco IOS se cifran usando el esquema débil, reversible usado para las contraseñas del usuario.

Para determinar qué esquema se usó para cifrar una contraseña, verifique el dígito que antecede a la cadena cifrada en el archivo de configuración. Si ese dígito es un 7, la contraseña ha sido cifrada utilizando el algoritmo débil. Si ese dígito es un 5, la contraseña ha sido codificada utilizando el algoritmo MD5 más fuerte.

Por ejemplo, en el comando de configuración:

```
enable secret 5 $1$iUjJ$cDZ03KKGh7mHfX2RSbDqP.
```

Se ha generado enable secret con MD5, mientras que en el comando:

```
username jdoe password 7 07362E590E1B1C041B1E124C0A2F2E206832752E1A01134D
```

La contraseña ha sido cifrada mediante un algoritmo reversible débil.

Archivos de configuración

Cuando envía información de la configuración por correo electrónico, debería vaciar la configuración de contraseñas de tipo 7. Puede usar el comando show tech-support, el cual vacía la información de forma predeterminada. **El show tech-support command output de la** muestra se muestra abajo.

```
username jdoe password 7 07362E590E1B1C041B1E124C0A2F2E206832752E1A01134D
```

Al guardar sus archivos de configuración en un servidor de Protocolo trivial de transferencia de archivos (TFTP), cambie los privilegios de ese archivo cuando no lo esté usando o colóquelo detrás de un firewall.

¿Se puede cambiar el algoritmo?

Cisco no tiene ningún plan inmediato para soportar un algoritmo de encripción más fuerte para las contraseñas del usuario del Cisco IOS. Si Cisco decide a introducir tal característica en el futuro, esa característica impondrá definitivamente una carga administrativa adicional ante los usuarios que eligen aprovecharse de ella.

No está, en el caso general, posible cambiar las contraseñas del usuario al Maryland - el algoritmo basado usado para los secretos del permiso, porque el MD5 es un troceo unidireccional, y la contraseña no se puede recuperar de los datos encriptados en absoluto. Para soportar ciertos Protocolos de autenticación (notablemente GRIETA), el acceso de las necesidades del sistema al texto claro de las contraseñas del usuario, y por lo tanto debe salvarlas usando un algoritmo

reversible.

Los problemas de administración de claves hacen que esto sea una tarea importante para cambiarlo a un algoritmo reversible tal como DES. Aunque fuera fácil modificar el Cisco IOS para utilizar el DES para cifrar las contraseñas, no habría ventaja en cuanto a la seguridad de este modo si todos los sistemas del Cisco IOS utilizaron la misma clave DES. Si distintos sistemas utilizaran claves distintas, se introduciría una carga administrativa para todos los administradores de red y se dañaría la capacidad de transferencia de archivos de configuración entre los sistemas. La demanda de un encripción de contraseñas reversible más fuerte por parte del cliente ha sido pequeña.

Información Relacionada

- Procedimientos para Recuperación de Contraseñas
- Guía de Cisco para endurecer los dispositivos Cisco IOS
- Soporte Técnico - Cisco Systems